Notice of Allowability	Application No.	Applicant(s)	
	09/630,711	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *23 August 2007*.

2. ☒ The allowed claim(s) is/are *1-31*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. This is in response to the communications filed on 23 August 2007.

2. Claims 1-31 are pending in the application.

3. Claims 1-31 have been allowed.

Response to Arguments

4. Applicant's arguments, see pre-appeal brief, filed 23 August 2007, with respect to claims 1-31 have been fully considered and are persuasive. The rejection of the claims has been withdrawn.

Allowable Subject Matter

5. Claims 1-31 are allowed.

The following is an examiner's statement of reasons for allowance:

The current application is directed towards the bread pudding protocol. The bread pudding protocol represents a novel use of proofs of work and is based upon the same principle as the dish from which it takes its name, namely, that of reuse to minimize waste. Whereas the traditional bread pudding recipe recycles stale bread, our bread pudding protocol recycles the '"stale" computations in a POW to perform a separate and useful task, while also maintaining privacy in the task. In one embodiment of the bread pudding protocol, the current application considers the computationally intensive operation of minting coins in the MicroMint scheme of Rivest and Shamir and demonstrate how the minting operation can be partitioned into a collection of POWs, which are then used to shift the burden of the minting operation onto a large group of untrusted computational devices. Thus, in accordance with one illustrative embodiment

of the current application, the computational effort invested in the POWs are recycled to accomplish the minting operation.

The closest prior art to the current application was Rose et al U.S. Patent No. 6,944,765 B1 (hereinafter Rose). Rose is directed towards a method of authenticating anonymous users while reducing potential for "middleman" fraud includes the step of constructing a puzzle in response to information received from a software user. The puzzle includes the received information. The puzzle is sent to the user by a software provider. The user solves the puzzle and returns the solution to the provider. The puzzle includes a portion of a value derived from an encrypted "cookie" and an exponentiation of the derived value. The cookie includes information about the user.

However, Rose differs from the current application in several aspects. Rose discloses a method of preventing a person from impersonating a plurality of users of software. The method advantageously includes the steps of constructing a plurality of puzzles, each puzzle having a solution that includes information about a respective one of the plurality of users, each puzzle requiring consumption of a resource to solve; and sending each puzzle to a respective one of the plurality of users for solution. There is no distributed computational task being accomplished in the Rose reference. The task is individual to the user. In fact, all claims state explicitly that the goal is to authenticate users of soft-ware, not to distribute a computational task among them. Rose fails to disclose distributing a computational task among a plurality of entities. Rose discloses the user returns the puzzle to the provider at a later time, as described at column 3, lines 13 -15. In contrast, Jakobsson discloses a Prover demonstrates a certain amount of computation has been performed within a specified interval of time as described in Jakobsson at page 5, lines

10 -15. Rose fails to disclose an entity demonstrating a certain amount of computation has been performed within a specified interval of time. Rose discloses the Provider receives the answer to a puzzle from a user, and not from one of a plurality of users because the puzzle includes user information, as described at column 3, lines 2-13. In contrast, Jakobsson discloses a first entity receives response from a second entity based on the response from several third entities, as described at page 3, lines 17- 23. Rose fails to disclose a first entity receiving a response compiled from more than two entities. Rose discloses a software distributor distributes software to a user solving a puzzle provided by the distributor. The puzzle is user specific, as described in Rose at column 2, lines 27-32. In contrast, Jakobsson at page 4, lines 3-7 discloses a POW can be recycled to other entities as a bread pudding protocol. Rose fails to disclose recycling a puzzle of a user to another user. Summarizing, Rose addresses an authentication problem by a user solving a user specific puzzle which is not recyclable by a provider. In contrast, Jakobsson discloses an entity or prover solving an authentication problem, via a plurality of entities in behalf of the prover demonstrating performance of a computational task within a specified time interval as a Proof of Work (POW). The POW is recyclable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy AM
November 14, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100